

Responsive Parameter based an AntiWorm Approach to Prevent Wormhole Attack in Ad hoc Networks

Vrutik Shah¹ and Dr.Nilesh Modi²

¹ Research Scholar, Department of Computer Science,
Karpagam Univerisity,Coimbatore,India,Sr.Asst.Professor,Indus University,Ahmedabad

Email: vrutikshah@yahoo.com

²Professor and Head,S.V. Institute of Computer Studies,Kadi, Gujarat, India

Email: drnileshmodi@yahoo.com

Abstract— The recent advancements in the wireless technology and their wide-spread deployment have made remarkable enhancements in efficiency in the corporate and industrial and Military sectors The increasing popularity and usage of wireless technology is creating a need for more secure wireless Ad hoc networks. This paper aims researched and developed a new protocol that prevents wormhole attacks on a ad hoc network. A few existing protocols detect wormhole attacks but they require highly specialized equipment not found on most wireless devices. This paper aims to develop a defense against wormhole attacks as an Anti-worm protocol which is based on responsive parameters, that does not require as a significant amount of specialized equipment, trick clock synchronization, no GPS dependencies.

Index Terms—Wormhole Attack, MANETs, Routing Security

I. INTRODUCTION

Ad hoc is originally a Latin word that literally means “for this purpose only”. These Wireless ad-hoc networks are self-possessed of sovereign nodes that are self- managed devoid of any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can effortlessly link or abscond the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes conversing with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV[1] (Ad-hoc On-Demand Distance Vector) in category of reactive protocol[1][2], DSR (Dynamic Source Routing) and DSDV (Destination- Sequenced Distance-Vector).

In ad hoc networks one of the most challenging attacks to defend against is the wormhole attack. In a sophisticated version of this attack, the attacker will copy all the control and selected data packets from one location in the network and almost simultaneously replay them at another location in the network. The attacker’s nodes do not need to share any credentials (IDs or keys) with nodes in the network as they can just copy the encrypted or signed packets and replay them. The two locations will be several hops away from each other, but will be connected through a high-speed wired or

wireless link controlled by the attacker. Obviously, the goal of the attacker is not to improve the network connectivity by helping connecting far away nodes, but to draw traffic through the wormhole.

The wormhole attack can be launched regardless of the MAC, routing, or cryptographic protocols used in the network and is thus difficult to defend against. Defense mechanisms against this attack are either very complex or very expensive. Most of the wormhole defense mechanisms aim to detect wormholes successfully with minimal false positives. Unfortunately, the defense schemes ignore the removal of the links created by the wormhole. We note that a single two-end wormhole could be thought of logically as a single link. In reality, the wormhole creates a large number of links between many nodes in the network. The nodes will not be aware of this fact and will be using the wormhole links as legal links. In this paper, we will discuss the potentially catastrophic impacts of the wormhole attack in more detail.

II. WORMHOLE ATTACKS AND ITS CLASSIFICATION

Wormhole attack is one of the most sophisticated forms of routing attacks in MANET. In this attack, an attacker records packets at one location, tunnels them to another location of the network, where it is retransmitted by a colluding attacker. The tunnel can be established by using either out-of- band private link (e.g., a wired link, or a long-range wireless transmission), or logical link via packet encapsulation. As a result, the tunneled packets arrive either sooner or with less number of hops compared to the packets transmitted over multi-hop routes. Based on the tunneling mechanism they use, wormholes can be classified into the following categories:

- i. Out-of-band wormhole
- ii. In-band wormhole

Before we discuss the implications of wormholes in MANET, the major differences between in-band and out-of-band wormholes are listed below:

- a. In an out-of-band wormhole, the colluders create a direct link between the two end-points, whereas in-band wormhole does not use any external communication medium.
- b. Out-of-band wormhole requires special hardware to support the communication between the two end-points. On the other hand, in- band wormhole does

- not require any special hardware or special routing protocol.
- c. In out-of-band wormhole, the tunneled packets arrive faster than the multi-hop packets, but the in-band wormhole works much slower create the illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors.
 - d. In-band wormhole attack can be launched easily by any node in the network to another colluder or a set of colluders which may include one or more relay nodes. So, in-band wormholes are more likely to be used in real adversaries.
 - e. Out-of-band wormhole adds channel capacity to the network, whereas in band wormhole consumes network capacity and thereby causes internal service degradation [13].
 - f. In both forms of wormhole attack, the attackers can tunnel packets which are not even addressed to them [12]. They can do so even if the network provides confidentiality.

Since in-band wormhole attack is simple to be implemented, it is more likely to take place in real life scenarios. In this research project, our focus is on detecting in-band wormhole attack in MANET. So, in this dissertation, we use the terms “in-band wormhole attack”, “wormhole attack”, and “traditional wormhole attack” for the same meaning.

Wormhole could be a useful networking service while it provides a long link to the link layer [3]. However, the adversaries may use the wormhole link for their own purposes. The existence of wormhole links can disrupt the routing service in a number of ways. The attackers can attract a significant amount of traffic from their surroundings. If the attackers keep the wormhole tunnel active at all times and do not drop any packets, they would actually perform a useful service for the network [4]. But they can be responsible for disrupting the data flow by selectively dropping or modifying packets, generating unnecessary routing activities by turning off the wormhole link periodically, and recording packets for later analysis. In Fig. 1.1 and Fig. 1.2, a two-hop wormhole attack scenario is presented, where W1 and W3 are the main attackers and W2 acts as a relay node. The attackers W1 and W3 encapsulate RREQs received from the nodes in their vicinity, and then forward them to the tunnel node W2. The attackers de-capsulate the packets received from the relay node W2, and then rebroadcast them in their vicinity. For example, RREQs from nodes D and L will be tunneled from W3 to W1 and then rebroadcasted by W1 and received by nodes E, C and S. These nodes will reply with RREP to acknowledge the RREQ. As a result a source node, for example S, will select a route to a destination (e.g. node D) which passes through the wormhole tunnel.

This chapter discusses previous work on preventing wormhole attacks. All protocols in this section fall under two broad categories: localization schemes and packet leases.

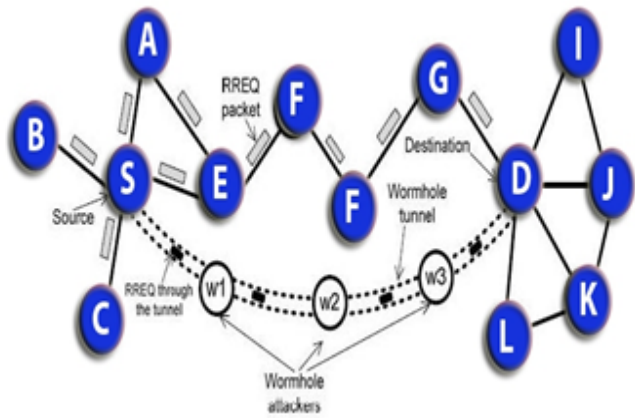


Figure 1.1 Path of RREQ packets (S->D) in presence of wormhole tunnel

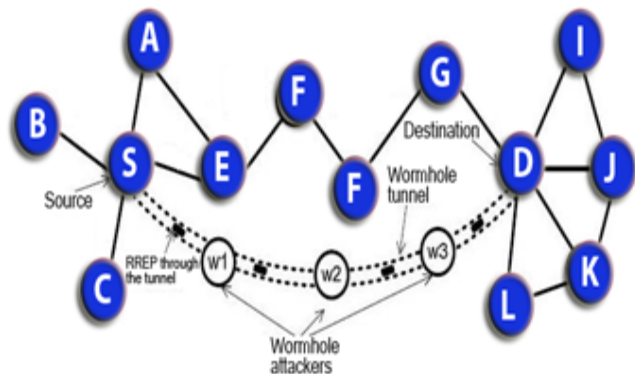


Figure 1.2 Path of RREP packets (D->S) in presence of wormhole tunnel

III. LITERATURE SURVEY: BACKGROUND WORK

A. Localization Schemes

Wireless security protocols based on localization have the potential to detect wormhole attacks [6,8,9]. Localization systems are based on verifying the relative locations of nodes in a wireless network [9,6,8]. Knowing the relative location may help conclude whether or not packets are sent by either a node or wormhole. Several localization schemes discussed in this section: Echo Protocol, Area-based Point Triangulation Test (APIT), Coordinate System, Signal Strength and Infra-Red (IR), and Directional Antennas. Sastry, Shankar and Wagner from the University of California at Berkeley discuss a location verification scheme known as the Echo protocol [4,10]. Rather than focusing on individual nodes of a network, this protocol emphasizes the regions of verification [10]. Nodes in the regions of verification must prove they are part of the wireless network using radio frequency (RF) and ultrasonic sound capabilities [10,9]. A verified node sends a RF signal to an unverified node in the network. To prove it is part of the network, the unverified node sends an ultrasonic signal back to the verified node. The verified node determines whether or not the unverified node is in the region of verification depending on the time it takes to receive an ultrasonic signal. RF signals are used in most wireless network devices today. The strong points of this protocol are that cryptography and tight time-synchronization are not needed.

However, because each network device needs additional equipment to detect and emit ultrasonic sound frequencies, this protocol may detract some developers from adopting this idea to prevent wormhole attacks. He, Huang, Blum, Stankovic and Abdelzaher developed an area-based point in triangulation test (APIT) which uses triangulation to determine the location of nodes in a network [9,11]. Calculations are performed to check whether or not certain nodes are within triangles formed by anchors, which are nodes with Global Positioning System (GPS) [9,10]. These calculations determine the relative locations of all nodes in the network which may prove helpful to combating wormhole attacks. Compared to the Echo protocol, APIT does not require additional equipment for ultrasonic sound frequencies. However, APIT does require some nodes to have GPS in the wireless network to give some reference of locations in a network so that nodes without GPS have a relative idea of where they stand [11].

Another localization scheme known as the coordinate system involves the work done by Nagpal, Shrobe and Bachrach at Massachusetts Institute of Technology (MIT) [14]. Similar to the APIT, the protocol uses a subset of GPS nodes to provide nodes without GPS a sense of relative location [14]. This is achieved using two algorithms: the gradient which measures a GPS node's hop count from a point in a network, and multilateration, which determines the way GPS nodes spread information of its location to nodes without GPS [14,4,5]. Hop counts tell how far a node is from a particular source. A flaw in using this scheme is that wormholes can disrupt hop counts within a network [5: 2]. Therefore, any system following this scheme is rendered defenseless under wormhole attacks.

Bulusu, Heidemann and Estrin discuss other localization techniques such as the verification of signal strength and Infra Red (IR) [11]. Weaker signal strengths may indicate a node is farther away. However, signal strengths are not reliable outdoors because ambient sound can disrupt signals-[11]. IR is very efficient in pinpointing nodes in open spaces using invisible lasers. On the other hand, IR is very sensitive to its surroundings rendering it unusable outdoors due to the interference of sunlight and indoor areas which do not have a line-of-sight to each network device [1: 3].

Hu and Evans developed a protocol using directional antennas to prevent wormhole attacks [6]. Directional antennas are able to detect the angle of arrival of a signal [6]. In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e. one from west and the other at east). This protocol falls only if the attacker strategically placed wormholes residing between two directional antennas. This problem has been solved by having a verifier check on the communications between two nodes [5: 8]. However, some legitimate nodes are invalidated due to this solution. Drawbacks to this protocol include the flaw of rejecting valid nodes and requiring the use of directional antennas to prevent wormhole attacks.

Overall, localization schemes are very effective in

determining location. Wormholes, which fake their location to appear to be in two or more places at once, may trigger protocols to reject them as invalid nodes.

B. Packet Leashes

Hu, Perrig and Johnson developed protocols with packet leashes have been proven to be reliable wormhole attack detectors [7]. Packet leashes place restrictions on a packet's maximum allowed transmission distance in a network [7,6]. Two types of packet leashes discussed in this article are temporal and geographical leashes. Temporal leashes require tightly synchronized clocks on all nodes [7]. Protocols based on temporal leashes ensure that packets transmitted across the network have an upper bound on its lifetime, which restricts the maximum distance of travel. Packets on a network remain valid for a certain time interval before they are rejected. However, setting up wormhole attacks under temporal leashes is difficult because packets must be sent through the wormhole within the restricted time period.

A geographical leash is the second type of leash discussed. Protocols based on geographical leashes differ slightly from temporal leashes in that each node must know its location and have loosely synchronized clocks [7]. Using location and time, nodes can determine whether the packet is coming from a valid node or a wormhole. This protocol allows more flexibility in the synchronization time among nodes than temporal

leashes [7]. This type of packet leash also incorporates some of the same ideas used in localization schemes of using location to prevent wormhole attacks.

A more refined temporal leash protocol known as the TESLA with Instant Key disclosure (TIK) is discussed by Hu, Perrig and Johnson. TIK uses a hash tree to hold symmetric keys to authenticate nodes. Receiving nodes will be able to determine a packet's validity based on the time interval and the corresponding key of the sender node]. TIK packets are structured so that the receiver node verifies the time interval and message authentication codes (HMAC) before the key arrives. If the time interval is valid, then the node verifies the key. Completing both tests would verify the sender was not a wormhole. The TIK temporal leash protocol effectively detects a majority of wormholes. An attacker must know the right time intervals and keys pairs so that nodes in the wireless network will accept the wormhole's packet. A disadvantage of this protocol is its strict requirements in timing. Each node must be synchronized at exactly the same time and errors in time difference must not be larger than a few microseconds or even hundreds of nanoseconds.

C. Conclusion

Protocols based on localization schemes and packet leashes can prevent wormhole attacks. However, each protocol has different costs in achieving this goal. As mentioned before, temporal leashes require strict time synchronization among all nodes. As a result, this project focuses more on localization schemes and geographical leashes because it does not require tight time

synchronization. However, the trade-off is that localization schemes and geographical leases tend to use additional hardware resources [16]. Many researchers deposited efforts to mitigate the wormhole attack. F. Nait-Abdesselam and T. Tarik have proposed techniques be applied to suspicious links [17] by means of an exchange of encrypted probing packets between the two supposed neighbors. A. Pirzada and C. McDonald has proposed trust based [18] schemes to combat with wormhole attacks. Buttyan, L. Dora, and I. Vajda proposed Statistical based approach [19] and W. Znaidi, M. Minier, and J.-P. Babau has proposed a local information based approach [20] to combating wormhole. Transmission time-based mechanism [23] has been proposed by P. V. Tran, L. X. Hung, Y.-K. Lee, S. Lee. WORMEROS framework [21] proposed by H. Vu, A. Kulkarni, K. Sarac, and N. Mittal. H. S. Chiu and K.-S. Lui proposed a detection method called delay per hop indication [22]. By observing the delays of different paths to the receiver.

IV. PROPOSED SOLUTION: DESIGN CRITERIA

In this paper, we propose “Anti-Worm”, a novel, yet straightforward protocol to effectively detect wormhole attacks. We make use of routing discrepancies among neighboring nodes along a path from a source to the destination to detect wormhole attacks. The protocol is simple and localized, can be applied on demand (when the existence or lack thereof of a wormhole needs to be verified) and needs no special hardware, localization, or synchronization. Thus Anti-worm can detect physical layer wormholes.

This protocol design as per decisions to meet certain goals. These goals were to design a protocol that prevents wormhole attacks

A. evade using strict clock synchronization.

Using strict clock synchronization to detect wormhole attacks is completely unrealistic. It necessitate all nodes to synchronize within a few microseconds or hundreds of nanoseconds, which rivets the utilize of highly sensitive and costly network devices., localization schemes and geographic leases[7] can be used to avoid strict clock synchronization. Therefore, design decisions of this protocol are based on detecting wormholes using relative location rather than timing constraints.

B. The need for specialized equipment.

Limiting the use of specialized equipment reduces the cost of creating a secure wireless network. Rather than requiring all nodes to have specialized equipment, this protocol uses a combination of GPS and non-GPS nodes to prevent wormhole attacks. Non-GPS nodes are equivalent to many nodes available off the ledge.. GPS nodes on the other hand would have all the properties of a non-GPS node except for the GPS. GPS were determined to be a low cost yet highly beneficial system compared to the use of other specialized equipment such as RF, IR and ultrasonic waves.

C. Ensures information confidentiality.

While providing protection against wormhole attacks is the primary goal, this protocol has minor goals to provide information confidentiality and integrity in addition to performance, power conservation and minimal data storage. The following paragraphs will discuss the designs of GPS, non-GPS nodes and the network environment for this protocol to achieve these goals.

V. PROPOSED SOLUTION: BASIC DESIGN

The example in Figure 2.1 summarizes the idea of the Anti-Worm protocol. Here the source has a short route (the route in red color) to the destination that goes through the wormhole. The goal of Anti-worm is to find alternative route that does not go through the wormhole (the route in green color). The source will check the difference between the two routes and if this difference is greater than some value that we will refer to as the Responsive parameter then a wormhole is detected.

That Means Rout1-Route2 Must be 2 or 3 Here in this example one route having 7 hop Count and another is having 3 hop count hence In this case the difference is $7-3=4$, we will use a Responsive parameter as 2 or 3.

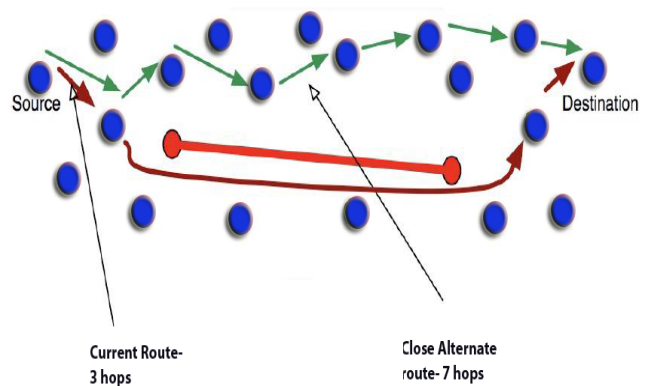


Figure 2.1 Design Idea of Antiworm Protocol

The difference is some how related to the length of the wormhole in number of hops. This explains why 2 or 3 is a good choice for the Responsive parameter. Note that by definition wormholes are longer than 1 hop (at least 2 hops). In fact the attacker wants to make the wormhole as long as possible because the longer the wormhole the healthier the attack since it will exert a pull on more traffic and will have bigger impact.

Network Topology depicted in figure 2.2, Based upon Design Criteria mentioned in above section like strict clock synchronization, Specialized equipment and Confidentially algorithm has been designed as depicted in fig 2.2 and pseudo code as bellowed.

Detection (A,B)

1. Based Upon GPS or Non GPS A finds N_A
2. B sends N_B to A
3. A chooses $T \in \{N_B - N_A\}$

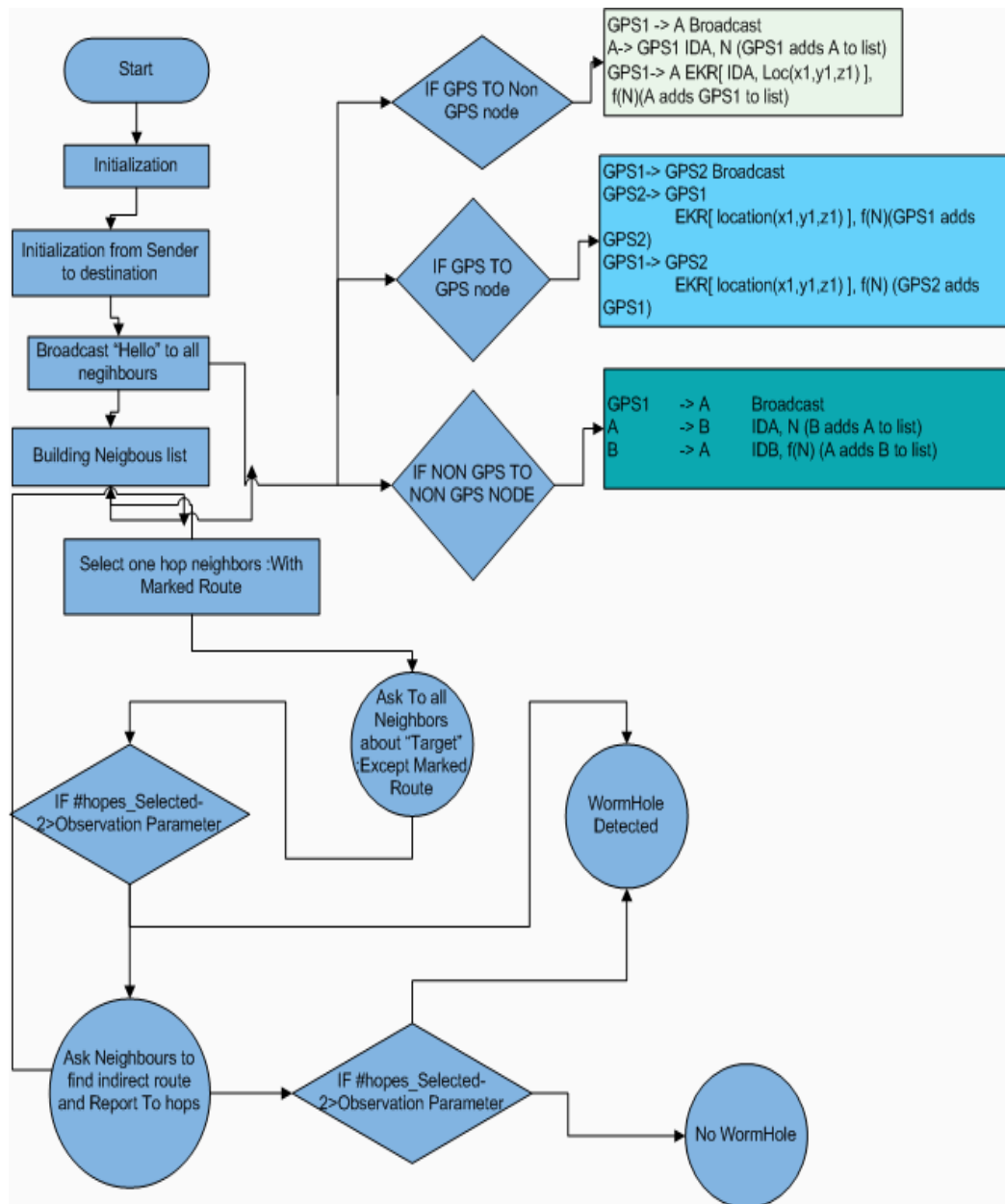


Figure 2.2 Flow Chart of Antiworm Protocol

4. $\forall X \in N_A$, X finds R_X "T : $N_B \cup N_A$ $f \subset R_X$ "T and $|R_X - T| > 1$
5. $\forall X \in N_A$, X sends $|R_X - T|$ to A
6. A determines $Select(R_X - T)$ and computes $|R_S - T|$
7. If $|R_S - T| > \eta + 3$ then A assumes B is connected to it through a wormhole

A flow chart of the Anti-Worm protocol is shown in Fig.2.3. We discuss the steps in the flowchart below. Consider a source node S that wants to communicate with destination node D and wishes to test for a wormhole. Let $u, v, x \in P_{SD}$ —they are nodes on the path from S to D that was obtained by using some standard routing protocol. Let the wormhole

A flow chart of the Anti-Worm protocol is shown in Fig.2.3. We discuss the steps in the flowchart below. Consider a source node S that wants to communicate with destination node D and wishes to test for a wormhole. Let $u, v, x \in P_{SD}$ —

©2014 ACEEE
DOI: 01.IJNS.5.1.8

they are nodes on the path from S to D that was obtained by using some standard routing protocol. Let the wormhole

$M1 \leftrightarrow M2$ connect nodes u and v where $u \in BM1$ and $v \in BM2$. Let x be the next hop from v on the route from S to D . Note that u and v are typically separated by several hops, but now will believe that they are neighbors.

The "Sender" node S will set the target node to be the node two hops away along the path, i.e., $T = P_{SD}^2$ initially. Let us suppose that node S wants to communicate with node D and the shortest path provided by some standard routing protocol is $(S - A - B - C - E - D)$. Note that there are five hops to the destination. Obviously this route passes through the wormhole and nodes B and C are connected through the wormhole transceivers $M1$ and $M2$ without being aware of this fact.

S will discover all its one-hop neighbors B_s by

broadcasting a “hello” message. The nodes in BS will hear the hello message and will reply to S. here for Preserving the confidentiality depends upon GPS or Non GPS node

1. GPS to Non GPS Node

- i. $GPS1 \rightarrow A$ Broadcast
- ii. $A \rightarrow GPS1$ IDA, N (GPS1 adds A to list)
- iii. $GPS1 \rightarrow A$ EKR[IDA, location(x1,y1,z1)], f(N) (A adds GPS1 to list)

2. Building neighbor list of GPS nodes

- i. $GPS1 \rightarrow GPS2$ Broadcast
- ii. $GPS2 \rightarrow GPS1$ E K R [location(x1,y1,z1)], N (GPS1 adds GPS2)
- iii. $GPS1 \rightarrow GPS2$ E K R [location(x1,y1,z1)], f(N) (GPS2 adds GPS1)

3. Building neighbor list of non-GPS nodes

- i. $GPS1 \rightarrow A$ Broadcast
- ii. $A \rightarrow B$ IDA, N (B adds A to list)
- iii. $B \rightarrow A$ IDB, f(N) (A adds B to list)

Based upon communication mode S will create a list of the nodes in BS and marks node P_{SD}^1 . Note that node P_{SD} and is known during route discovery to the destination D.

Now, S will broadcast the list (B_s, T) and ask every node $q \in \{B_s - P_{SD}\}$ to find a route to target node T, such that the route does not include any other node in B_s (will be referred to as forbidden list). That is $\nexists q, z \in B_s$ where $q = z$. AntiWorm ensures that $z \in Pq, T$. Each node $q \in \{B_s - P_{SD}\}$ will run the network routing algorithm and reply to S with lqT , the length (in number of hops, or the cost) of its route to T. If lqT does not exist due to the connectivity of the network topology then q will inform S and S discards q from $\{B_s - P_{SD}\}$.

The second calculation determines whether two nodes can communicate with each other. For example, suppose there are two nodes A and J that are within the transmission radius of each other. If the distance between any GPS node in node A's neighbor list and any GPS node in node J's neighbor list is greater than three times the transmission radius of the node, then both nodes are most likely subjected to a wormhole attack. A node can only communicate with another node with the maximum distance of the GPS nodes at the end of their transmission radii as illustrated in Figure 3.1. This calculation will be referred as the two-hop calculation.

To summarize, nodes that fail the one-hop calculation are likely to be nearby a wormhole. Nodes that fail the two-hop calculation are potentially sending packets to a node compromised by a wormhole. In the detection process, any node failing the one-hop and two-hop calculations shut down and are removed to avoid additional damage on the network. The next chapter will show how these processes were implemented and simulated to model realistic network conditions. To Maintain confidentiality in Communication Process Communication via non-GPS nodes

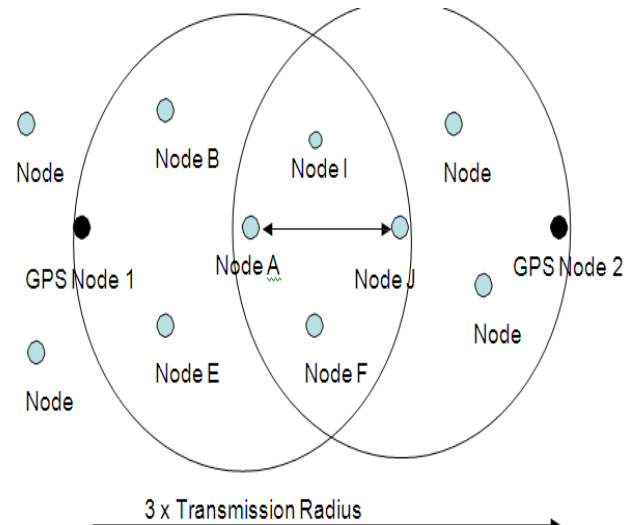


Figure 3.1 Transmission Range Antiworm Protocol

- i. $A \rightarrow B$
 $KAB[IDA, IDC, A's GPS List, KAC[data]], N$
- ii. $B \rightarrow C$
 $KBC[IDA, IDC, B's GPS List, KAC[data]], f(N)$

Communication via GPS nodes

- i. $A \rightarrow GPS1$
 $IDA, IDC, A's GPS List, KAC[data], N$
- ii. $GPS1 \rightarrow C$
 $EKR[IDA, IDC, location(x,y,z), KAC[data]], f(N)$

Node C verifies f(N) and decrypts to receive message. For Detection process if there is a one hop calculation for Distance A's nearby transmission radius for GPS1 and GPS2, in case of one hop category it must be lesser than transmission range of A's multiply by 2. If there are multiple hops like A and B then A's GPS and B's GPS distance must be lesser than transmission range of them multiply by 3 if Observation parameter is more than 3 than wormhole detected in the network. In order to prevent that all node broadcast to each one about wormhole nodes.

VI. OVERHEAD ANALYSIS OF ANTI-WORM

In this section of paper we discuss the overhead analysis if anti-worm is used. For this we utilize a model of network with parameters like Size of Network, Number of nodes and its transmission range to determine the average number of packets that need to broadcast by sender, the number of route acquisitions performed by nodes to target node implies directly with reply packets.

We start with the number of nodes that need to become “senders” to check for the wormhole until it is detected. This equals the number of broadcast messages and this number depends on the number of hops between the sender and the destination and the position of the wormhole.

Let us suppose that nodes are uniformly and randomly distributed in a square area of size X^2 . Nodes can communicate directly if the distance between them is less than the transmission range R. Let $d_{i,j}$ be the distance between two nodes i and j. Let $N_{i,j}$ be the number of hops of the

shortest path between nodes i and j . Then

$$\text{Min}(NSD) \text{ as } N_{s,D} \geq d_{s,D}/R \text{ and,} \\ N_{s,D} = \beta d_{s,D}/R, \text{ where } 1 \leq \beta \leq 2.$$

Let M1 and M2 be the transceivers of the wormhole located somewhere between S and D. The wormhole will be detected when the latest “sender” along the route is located within M1’s range. In the best case M1 could be a neighbor of S and thus detected immediately. In the worst case M1 could be two hops away from D (M2 is D’s neighbor – we assume that the special case in Section 3.3 is identical to other cases but it requires a few extra messages). Thus, on average, the number of “senders” that need to check for the wormhole will be:

$$N_{check} = (\beta d_{s,D}/R - 2)/2 = (\beta d_{s,D}/2R) - 1 \quad (1.1)$$

With a square area of size X^2 , the longest distance between S and D can be “2A. This happens when the sender and destination are located at two opposite corners diagonally. The maximum number of sender nodes that need to check for the wormhole before the wormhole is detected N_{check} is:

$$N_{check} = (\sqrt{2\beta A/2R}) - 1$$

The probability of having k number of neighbors within the transmission range R of a node can be derived as in [15]:

where N is the total number of nodes in the network. Thus the average number of neighbors will be:

$$AV_k = k \cdot P(k) = N \cdot \pi \cdot R^2/A^2 \quad (1.2)$$

For a given X , R , and N , the number of packets that need to be broadcast by sender nodes is given by (1.1). We show that this is not a significant overhead use the number of route acquisitions given by (1.2) with the parameters of the simulated network and $\beta = 1$ and $\beta = 1.5$, to define a lower and upper bound for the number of route acquisitions.

VII. CONCLUSION & FUTURE WORK

The wormhole attack was presented in particular details, providing definitions, defining the different types, and explaining the potential impact of such attacks. Neighbor discovery in ad hoc networks was discussed. Classification for secure neighbor discovery and wormhole detection protocols was presented. The classification was based on the techniques and the approaches the protocols used. The available detection and secure neighbor discovery protocols in the literature were described with clarification of the main issues with each Wormhole attacks are significant problems that need to be addressed in wireless network security. Although substantial research has been done to combat wormhole attacks, this protocol is to proposed a collaboration of GPS and non-GPS nodes as an aid to prevent this type of attack.

As a Future work we will simulate Anti-worm protocol in real time utilizing Network simulators for network performance parameter like Throughput, Good put, Packet delivery fraction and Route Discovery Time.

REFERENCES

- [1] C. E. Perkins, E. M. B. Royer and S. R. Das, “Ad-hoc On-Demand Distance Vector (AODV) Routing,” Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manet-aodv-00.txt, Feb. 2003.
- [2] Hao Yang; Haiyun Luo; Fan Ye; Songwu Lu; Lixia Zhang; , “Security in mobile ad hoc networks: challenges and solutions,” Wireless Communications, IEEE , vol.11, no.1, pp. 38- 47, Feb 2004.
- [3] R. Maheshwari, J. Gao, and S. Das. Detecting wormhole attacks in wireless networks using connectivity information. In Proceedings of INFOCOM ’07, May 2007, p. 107-115.
- [4] R. Poovendran and L. Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Networks, 2007. 13(1): p. 27-59.
- [5] Hu, Lingxuan and David Evans. “Using Directional Antennas to Prevent Wormhole Attacks.” Network and Distributed System Security (NDSS 2004), February 2004.
- [6] Hu, Lingxuan and David Evans. “Localization for Mobile Sensor Networks.” MobiCom 2004. 21 March 2004.
- [7] Hu, Yih-Chun, Adrian Perrig and David B. Johnson. “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks.” 23 October 2003. < www.monarch.cs.rice.edu/monarch-papers/tikreport.pdf >.
- [8] He, Tian, Chengdu Huang, Brain M. Blum, John A. Stankovic and Tarek Abdelzaher. “Range-Free Localization Schemes for Large Scale Sensor Networks.” Mobicom 2003. 23 October 2003 < www.cs.virginia.edu/~th7c/paper/APIT_CS-2003-06.pdf >.
- [9] Hu, Lingxuan. “Some Security Issues in Wireless Sensor Networks.” E-mail to the author. 23 October 2003.
- [10] Sastry, Naveen, Umesh Shankar, and David Wagner. “Secure Verification of Location Claims.” ACM Workshop on Wireless Security (WiSe 2003), September 19, 2003. 23 October 2003. < www.cs.berkeley.edu/~nks/locprove/csd-03-1245.pdf >.
- [11] Bulusu, N, J. Heidemann and D. Estrin. “GPS-less Low Cost Outdoor Localization for Very Small Devices.” IEEE Personal Communications Magazine, October 2000. 23 October 2003 < www.isi.edu/~johnh/PAPERS/Bulusu00a.pdf >.
- [12] Y. Hu, A. Perrig, and D. Johnson, Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications, 2006. 24(2): p. 370-380.
- [13] J. Baras, S. Radosavac, G. Theodorakopoulos, et. al., Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR. In Proceedings of Military Communication Conference (MILCOM ’07), 2007, p. 1-7.
- [14] Nagpal, Radhika, Howard Strobe and Jonathan Bachrach. “Organizing a Global Coordinate System from Local formation on an Ad Hoc Sensor Network.” 23 October 2003 < http://www.swiss.ai.mit.edu/projects/amorphous/papers/ipsn-2003-v5.pdf >.
- [15] I. Broustis, A. Vlavianos, P. Krishnamurthy, and S. Krishnamurthy, “Ctu: Capturing throughput dependencies in uwb networks,” INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp. 412–420, April 2008.
- [16] L. Qian, N. Song, and X. Li, “Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach,” J. Netw. Comput. Appl., vol. 30, no. 1, pp. 308–330, 2007, 1238698.
- [17] F. Nait-Abdesselam and T. Tarik, “Detecting and avoiding wormhole attacks in wireless ad hoc networks,” IEEE

- Communications Magazine, vol. 46, no. 4, pp. 127–133, April 2006.
- [18] A. A. Pirzada and C. McDonald, “Detecting and evading wormholes in mobile ad-hoc wireless networks,” *International Journal of Network Security*, vol. 3, no. 2, pp. 191–202, September 2008.
- [19] L. Buttyan, L. Dora, and I. Vajda, “Statistical wormhole detection in sensor networks,” in *In Proceedings of the Second European Workshop: Security and Privacy in Ad-hoc and Sensor Networks*, 2006.
- [20] W. Znaidi, M. Minier, and J.-P. Babau, “Detecting wormhole attacks in wireless networks using local neighborhood information,” in *Proc. of IEEE PIMRC*, 2008.
- [21] H. Vu, A. Kulkarni, K. Sarac, and N. Mittal, “Wormeros: A new framework for defending against wormhole attacks on wireless ad hoc networks,” in *In Proc. of the Third International Conference on Wireless Algorithms, Systems, and Applications*, 2008.
- [22] H. S. Chiu and K.-S. Lui, “Delphi: wormhole detection mechanism for ad hoc wireless networks,” in *In Proc. of the First International Symposium on Wireless Pervasive Computing*, 2006.
- [23] P. V. Tran, L. X. Hung, Y.-K. Lee, S. Lee, and H. Lee, “Ttm: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks,” in *In Proc. of IEEE CCNC*, 2007.

AUTHOR’S PROFILE

Vrutik Shah was born in India in 1980; He is a Ph.D scholar in Computer Science He received his MCA degree in Computer Science and Application. His research interest includes security in wireless networks, Ad- Hoc networks, and network protocols. He is working in Computer Science Department, Inuds University Ahmedabad. This work is a part of Ph.D Program from KARPAGAM University, Coimbatore, INDIA.

Dr. Nilesh Modi received his MCA from Hemchandracharya North Gujarat University in 2002, and his Ph.D. in computer science from Bhavnagar University in 2006. He is currently a Professor and Head of Department at SVICS, Kadi,